Notice of Allowability	Application No.	Applicant(s)	
	09/892,904	AUDEBERT ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment After Final Rejection*.

2. ☒ The allowed claim(s) is/are *86 and 94*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *8/8/07* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8,8,07

DETAILED ACTION

1. Examiner initiated interview has been made, to for unknown abbreviation "PSD" since the abbreviation has no-well recognized meaning in the field and leaves the reader in doubt as to the meaning of the technical features to which it refers, with James E. Ledbetter on 8/8/07. Based on the interview, Examiner's amendment has been made for independent claims 86.

2. This office action is in response to Amendment After Final Rejection filed on 07/30/2007. Claims 86 and 94 were previously allowed in the final action mailed 1/29/07. The office herein allows claims 86 and 94 in respond to the applicant's amendment. Claims 1-85, and 87-93, and 95-97 are cancelled.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with James E. Ledbetter on 8/8/07.

Claim 86 is amended as follows:

86 (Currently Amended) A method for generating a key protection certificate comprising:

injecting a first securely shared secret key, a second securely shared secret key, a key protection algorithm and cryptographic seed information into a ~~PSD~~ personal security device (PSD) which comprises a unique device name, wherein at least a portion of said seed information is used in generating at least one public key and one private key,

storing said injected first and second securely shared secret keys and said cryptographic seed information in a secure domain within said PSD,

sending a command to said PSD for generating said at least one public key and one private key, wherein said command initiates generation of said keys and of said key protection certificate,

generating said at least one public key and said one private key using at least a portion of said seed information, generating contextual attributes specific to at least the generation of said private key,

encrypting at least a portion of said contextual attributes using said first securely shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in said private contextual attributes,

storing said public key and said private key in said secure domain within said PSD,

generating a digital signature of said unique device name using said private key,

concatenating said unique device name, said private contextual attributes, said public contextual attributes with said digital signature and generating a first intermediate result,

generating a message authentication code of said first intermediate result using said second securely shared secret key producing a second intermediate result,

concatenating said first intermediate result with said second intermediate result producing said key protection certificate; and

storing said key protection certificate in said secure domain within said PSD.

Allowable Subject Matter

3. Claims 86 and 94 are allowed.

4. The following is an examiner's statement of reasons for allowance: The applied references neither alone nor in combination fail to teach the method for generating a key protection certificate comprising a personal security device generating at least one public key and said one private key using at least a portion of said seed information, generating contextual attributes specific to at least the generation of said private key, encrypting at least a portion of said contextual attributes using said first securely shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in the private contextual attributes, generating a digital signature of said unique device name using said private key and concatenating the unique device name, the private contextual attributes, the public contextual attributes with the digital signature and generating a first intermediate result, generating a message authentication code of the first intermediate result using the second securely shared secret key producing a second intermediate result and generating a key protection certificate by concatenating the first intermediate result with the second intermediate result.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

August 8, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8,8,07